WEST Search History

DATE: Thursday, April 03, 2003

Set Name side by side	**Query**	**Hit Count**	**Set Name** result set
DB=USPT; PLUR=YES; OP=ADJ			
L19	handshake and L18	10	L19
L18	cookie and l15	18	L18
L17	universal session manager and L14	0	L17
L16	universal session manager and L15	0	L16
L15	client and server and user and L14	99	L15
L14	authentica$5 and L13	107	L14
L13	remote and host and l11	141	L13
L12	remote 2a isp and L11	0	L12
L11	(isp or internet service provider) and L10	244	L11
L10	user same login	1618	L10
L9	network and L8	16	L9
L8	two-side$ and authentica$4	49	L8
L7	two-side$ same authentica$4	0	L7
L6	two-side$ 3a authentica$4	0	L6
L5	network and L4	2	L5
L4	authentication same two side$	12	L4
L3	l1 and network	2	L3
L2	cookie and L1	1	L2
L1	authentication same two side	12	L1

END OF SEARCH HISTORY

WEST

Generate Collection | Print

Search Results - Record(s) 1 through 10 of 10 returned.

☑ 1. Document ID: US 6523027 B1

```
L19: Entry 1 of 10          File: USPT          Feb 18, 2003

US-PAT-NO: 6523027
DOCUMENT-IDENTIFIER: US 6523027 B1

TITLE: Interfacing servers in a Java based e-commerce architecture
```

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. Desc | Image

---

☑ 2. Document ID: US 6502102 B1

```
L19: Entry 2 of 10          File: USPT          Dec 31, 2002

US-PAT-NO: 6502102
DOCUMENT-IDENTIFIER: US 6502102 B1

TITLE: System, method and article of manufacture for a table-driven automated
scripting architecture
```

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. Desc | Image

---

☑ 3. Document ID: US 6453353 B1

```
L19: Entry 3 of 10          File: USPT          Sep 17, 2002

US-PAT-NO: 6453353
DOCUMENT-IDENTIFIER: US 6453353 B1

TITLE: Role-based navigation of information resources
```

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. Desc | Image

---

☑ 4. Document ID: US 6335927 B1

```
L19: Entry 4 of 10          File: USPT          Jan 1, 2002

US-PAT-NO: 6335927
DOCUMENT-IDENTIFIER: US 6335927 B1
```

TITLE: System and method for providing requested quality of service in a hybrid network

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC
Draw Desc | Image

☑ 5. Document ID: US 6182142 B1

L19: Entry 5 of 10 File: USPT Jan 30, 2001

US-PAT-NO: 6182142
DOCUMENT-IDENTIFIER: US 6182142 B1

TITLE: Distributed access management of information resources

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

☑ 6. Document ID: US 6161139 A

L19: Entry 6 of 10 File: USPT Dec 12, 2000

US-PAT-NO: 6161139
DOCUMENT-IDENTIFIER: US 6161139 A

TITLE: Administrative roles that govern access to administrative functions

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

□ 7. Document ID: US 5999525 A

L19: Entry 7 of 10 File: USPT Dec 7, 1999

US-PAT-NO: 5999525
DOCUMENT-IDENTIFIER: US 5999525 A

TITLE: Method for video telephony over a hybrid network

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

☑ 8. Document ID: US 5963915 A

L19: Entry 8 of 10 File: USPT Oct 5, 1999

US-PAT-NO: 5963915
DOCUMENT-IDENTIFIER: US 5963915 A

TITLE: Secure, convenient and efficient system and method of performing trans-internet purchase transactions

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

□ 9. Document ID: US 5867495 A

L19: Entry 9 of 10 File: USPT Feb 2, 1999

US-PAT-NO: 5867495
DOCUMENT-IDENTIFIER: US 5867495 A

TITLE: System, method and article of manufacture for communications utilizing calling, plans in a hybrid network

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

□ 10. Document ID: US 5867494 A

L19: Entry 10 of 10 File: USPT Feb 2, 1999

US-PAT-NO: 5867494
DOCUMENT-IDENTIFIER: US 5867494 A

TITLE: System, method and article of manufacture with integrated video conferencing billing in a communication system architecture

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

Generate Collection | Print

Term	Documents
HANDSHAKE.USPT.	4988
HANDSHAKES.USPT.	605
(18 AND HANDSHAKE).USPT.	10
(HANDSHAKE AND L18).USPT.	10

Display Format: TI | Change Format

Previous Page Next Page

WEST Search History

DATE: Thursday, April 03, 2003

Set Name side by side	**Query**	**Hit Count**	**Set Name** result set
DB=USPT; PLUR=YES; OP=ADJ			
L11	triple handshake	2	L11
L10	triple handshake and authentica$4	0	L10
L9	triple handshake same authentica$4	0	L9
L8	handshake and L4	1	L8
L7	handshake and L5	0	L7
L6	three and L5	0	L6
L5	triple and L4	0	L5
L4	browser and L3	1	L4
L3	text and L2	1	L3
L2	id and L1	1	L2
L1	5963915.pn.	1	L1

END OF SEARCH HISTORY

WEST

End of Result Set

□ Generate Collection Print

L8: Entry 1 of 1 File: USPT Oct 5, 1999

DOCUMENT-IDENTIFIER: US 5963915 A
TITLE: Secure, convenient and efficient system and method of performing trans-internet purchase transactions

Abstract Text (1):
A purchase transaction is performed between a client browser and a merchant server over a general access wide area connected network. The transaction appears to the client as singularly identifying a purchasable product or service and singularly confirming the purchase. A persistent predetermined coded identifier is established on the client browser corresponding to an account record stored by the merchant server. A predetermined URL referencing a purchasable product or service is served to the client browser. The predetermined URL includes an implicit reference to the persistent predetermined coded identifier. The predetermined URL is received by the merchant server, including the predetermined coded identifier, in response to a client browser selection. The merchant server validates the predetermined coded identifier against the account record and records an identifier of the purchasable product or service as derived from the predetermined URL by the merchant server.

US Patent No. (1):
5963915

Brief Summary Text (5):
During the past few years, there has been a substantial growth in the quantity and diversity of information and services available over the Internet. The number of users of the Internet has similarly grown quite rapidly. Perhaps one if not the predominant area of growth on the Internet has been in the use of the World Wide Web, often referred to as WWW, W3, or simply "the Web." The hyper-text transfer protocol (HTTP) that serves as the foundation protocol for the Web has been widely adopted and multiply implemented in Web browsers and Web servers. Web browsers provide a convenient user application for receiving generally high quality text and graphical based information in a scrollable display page format. Such Web pages are related by embedded hyper-text links that reference other Web pages. Selection of a hyper-text link, either by direct reference or implied reference through an image map, causes a hyper-text jump to the selection referenced Web page. Selection is generally through a simple, single mouse click on a displayed portion of the text or graphics. This system of simply selecting relations makes browsing successive Web pages served from potentially quite diverse and distant Web servers convenient and intuitive, and accounts in large part to the rapid and wide acceptance of the Web as an information resource.

Brief Summary Text (6):
One of the anticipated uses of the Web has been to provide a venue for commercial transactions in products and services. However, commercial use of the Web has distinctly not met the anticipated potential for a number of reasons. These reasons include security, convenience of use, and efficiency. Regarding security, current conventional Web browsers generally provide for the use of a reasonably secure encryption protocol overlaid on the HTTP protocol. The encryption protocol, typically involving a key-exchange based encryption algorithm, permits individual transactions over the Internet to be secure. Consequently, sensitive information, such as credit card numbers and the like, can be reasonably transferred over the Internet with little risk that the information can be misappropriated and misused.

Brief Summary Text (7):
An exemplary security system utilized by conventional HTTP browsers and servers is known as the secure sockets layer (SSL). The secure sockets layer defines and implements a protocol for providing data security layered under various application protocols, such as HTTP in particular, and over a conventional TCP/IP communications stack. The secure sockets layer protocol discretely provides the potential for data encryption, server authentication, message integrity, and client authentication for supported protocol connections over a TCP/IP connection. In use, the secure sockets layer is implemented at both the client browser and server ends of a network connection. A conventional uniform resource locator (URL), utilizing "https" as the secure HTTP protocol identifier, is issued by the client browser to specifically request a secure client/server session. A series of handshake transactions are provided to negotiate the establishment of the secure session including performing an encryption key exchange that is used in an encryption algorithm implemented by both the client-side and server-side secure sockets layers.

Brief Summary Text (8):
As part of this handshaking, the client browser may also retrieve the authentication certificate of the server for validation against a known certificate authority to ensure that the server is not an imposter. The secure HTTP protocol permits the server to also request and validate the authentication certificate, if any, held by the client. However, in general, client browsers and, more specifically, their client host computer systems are rarely registered with a publicly accessible authentication certificate authority. Thus, general use of client certificate authentication is not a viable means for identifying specific client users or client computer systems.

Brief Summary Text (9):
As a consequence, commercial use of the Web to sell products and services practically requires the establishment of a forms based user identification scheme, typically based on user name and password, by the server system to securely identify and re-identify a specific client user. Providing the user name and password to initiate each purchase session with a particular server is the minimum required to authenticate the client user. The underlying secure HTTP protocol session ensures that the user name and password are securely transmitted in an encrypted form over the Internet to the correct server. By the fundamental nature of the key exchange encryption algorithm used, only the server can decrypt to clear text the user name and password provided from the client browser.

Brief Summary Text (10):
A secure HTTP session may span a number of individual HTTP transactions between a client browser and server. With each of these individual transactions, the exchange keys are in effect permuted synchronously by both the browser and server to vary the encryption coding used for each transaction. However, each established secure HTTP session requires definite closure to prevent a security breach commonly known as a "third party assumption of identity attack." That is, a third party may be able to continue the secure session started by another client browser relative to the server. Since client user authentication only occurs at the initiation of the secure session, the third party fully assumes the authorization of the session initiating client browser.

Brief Summary Text (12):
A facility known as persistent client-side cookies has been introduced to provide a way for server systems to store selected information on client systems. Cookies are created at the discretion of the server system in response to specific client URL requests. Part of the server response is a cookie consisting of a particularly formatted string of text including a cookie identifier, a cookie path, a server domain name and, optionally, an expiration date, and a secure marker. The cookie is automatically discarded by the client system based on the expiration date. If the secure marker is present, then the cookie is only returned to a server system during a secure transaction. Where a URL client request made by the client, the cookie paths and domain names of cookies stored by the client are compared with those of the URL request. Cookies with matching paths and domain names are passed with the client URL request to the server system. Any text associated with the identifier is

also passed back to the server system. In Internet purchasing applications, the identifiers and associated text can be used to store information about the current purchase selections.

Brief Summary Text (20):
This is achieved in the present invention by providing for a purchase transaction that appears to the client user as a singular selection of a purchasable product or service and a singular confirmation of the purchase. A persistent predetermined coded identifier is established on the client browser corresponding to an account record stored by the merchant server. A predetermined URL referencing a purchasable product or service is served to the client browser. The predetermined URL includes an implicit reference to the persistent predetermined coded identifier. The predetermined URL is received by the merchant server, including the predetermined coded identifier, in connection with a client browser selection. The merchant server validates the predetermined coded identifier against the server stored account record and records an identifier of the purchasable product or service as derived from the predetermined URL by the merchant server.

Brief Summary Text (22):
Another advantage of the present invention is that a purchase selection URL may be embedded in widely distributed hyper-text documents served by merchant vendors, vendor agents, distributors, electronic catalogers and the like while maintaining both transaction identity and transaction security and affording substantial transaction efficiencies.

Brief Summary Text (24):
Yet another advantage of the present invention is that server side automation can provides for automatic simultaneous purchase transaction handling for both secure and unsecure client browsers.

Drawing Description Text (3):
FIG. 1 illustrates a client/server system architecture providing for a hyper-text transfer protocol connection between client and server computer systems;

Detailed Description Text (2):
An Internet computer system 10 is generally illustrated in FIG. 1. A conventional client computer system 12, executing a client browser application that supports the HTTP protocol, is connected typically through an Internet Service Provider (ISP) to the Internet 14. A server computer system 16 is also coupled typically through an Internet Service Provider to the Internet 14. The server computer system 16, controlled by a local console 18, executes a Web server application conventionally known as a HTTPd server. In addition, the server computer system 16 preferably provides local storage for at least one, though typically many Web pages.

Detailed Description Text (4):
A "protocol.sub.-- identifier" of "http" specifies the conventional hyper-text transfer protocol. A URL request for a secure Internet transaction typically utilizes the secure protocol identifier "https," assuming that the client browser and Web server are presumed to support and implement the secure sockets layer. The "server.sub.-- path" is typically of the form "prefix.domain," where the prefix is typically "www" to designate a Web server and the "domain" is the standard Internet sub-domain.top-level-domain of the server system 16. The optional "web.sub.-- page.sub.-- path" is provided to specifically identify a particular hyper-text page maintained by the Web server.

Detailed Description Text (5):
In response to a received URL identifying an existing Web page, the server system 16 returns the Web page, subject to the HTTP protocol, to the client computer system 12. This Web page typically incorporates both textural and graphical information including embedded hyper-text links that permit the client user to readily select a next URL for issuance to the Internet 14.

Detailed Description Text (7):
A hyper-text link of this form directs the execution of the logon.cgi program on an HTTP server in response to a client side selection of an hyperlink. A logon form

supported by a logon CGI program is typically used to obtain a client user login name and password to initiate an authenticated session between the client browser and Web server for purposes of supporting, for example, a purchase transaction.

Detailed Description Text (12):
On recognition of the redirect key word, the second URL in the redirection URL is returned to the browser executing on the client system 12 as part of a redirection message that directs the browser to issue a new URL request consisting essentially of the second URL. As a result, the "data" portion of the direct URL is effectively delivered to the direct server for purposes of accounting and potentially also validation, while the second URL is issued to the redirect server essentially transparently to the client user.

Detailed Description Text (13):
Referring now to FIG. 2 a number of different scenarios are presented where the present invention is utilized in simple to complex purchase transactions that, at least from a client user's perspective, are all equally secure and convenient. Each, from the merchant vendor's perspective, is also quite efficient. In a first scenario, a Server-1 22 serves a Web page 24 to a client browser in response to a URL request/Web page service transaction T1. The Web page 24 may embed any number of hyperlinks including for example hyperlinks 26, 28, 30, 32. The hyperlink 26 may represent a direct reference to an embedded URL or an active image map that can be utilized to ultimately resolve a client user selection on a discrete portion of a displayed graphic to a specific URL. The image map representation can thus be utilized to provide multiple selectable choices regarding one or more products or services graphically depicted by the hyperlink 26. These different but related URLS preferably allow the client user to separately request further information about the indicated product or service, information regarding other related products and services, information regarding the availability, method of shipment and terms of purchase for the indicated product or service, and to directly issue a request to purchase the product or service.

Detailed Description Text (14):
Where the selection reflects a request for further information, an image map selection identifier is passed as part of a transaction T2 to a vendor Server-2 34. The Server-2 34 can be the same logical or physical server as Server-1 22 or a completely independent server. The requested information is returned to the client browser as part of the transaction T2 preferably in the form of a Web page. Where the image map selection is resolved to a request to purchase URL, the present invention preferably provides for the purchase URL to specify use of a secure HTTP session with the Server-2 34. In accordance with the secure protocol, such as implemented by the secure sockets layer, the Server-2 34 negotiates and establishes a secure session T2 with the client browser. Once the secure session is established, the purchase request URL is, at least in effect, issued to vendor Server-2 34. Any client-side stored cookie data that properly corresponds to the request URL is also passed to the Server-2 34. In the preferred instance where an authenticated credit relationship has been pre-established between the client user and the Server-2 34, the client-side cookie encodes information sufficient to re-authenticate the client user to the Server-2 34. Where a client/vendor credit relationship has not been pre-established, a corresponding cookie will not exist on the client system 12. In this case, the Server-2 34 may initiate a conventional process of establishing and validating a credit relationship with the client user. Preferably, the Server-2 provides a registration form to the client browser for display and completion by the client user as part of the secure transaction T2. The registration form typically provides for the entry of a name, a password, a credit card number, billing and shipping addresses for the client user and possibly other relevant information. The resulting information is used by the Server-2 34, in accordance with the present invention, to create and store a client-side cookie on the client system 12 for use in connection with a subsequent URL purchase request. A database record is also preferably created in the database 36.

Detailed Description Text (23):
The Server-3 38 returns a redirection message and the second URL to the client browser. As in the case of the purchase URL provided to the Server-2 34, the second URL of the redirection URL preferably specifies a secure protocol, such as "https,"

a specific Web server, such as Server-4 40, and includes a Web page path that can be used to identify a particular product or service. Thus, in response to the redirection message from Server-3 38, the client browser preferably autonomously operates to establish a secure session transaction T4 with the Server-4 40. The sensitive data provided by the client-side cookie that is selected specifically by the second URL of the redirection URL is therefore passed to the Server-4 40 within the secure session transaction T4. The secure purchase transaction T4 then completes in the same manner as described above with regard to transaction T2.

Detailed Description Text (32):
FIG. 3 provides a detailed flow diagram illustrating the operation of the present invention in the purchase of a product over the Internet 14. Initially, the client browser receives a Web page 50 having any number of embedded URLs, either directly or through an indirect reference provided by an image map. The client user selects 52 a product from the Web page for purchase. The client browser ascertains 54 the corresponding URL. Preferably, this product reference URL specifies a request for a secure HTTP transaction. If a secure transaction 56 can be established with the server specified by the product URL, the client browser will autonomously determine whether a cookie having a matching domain and path reference exists on the client system 12. In accordance with the present invention, such a cookie will be marked secure, to prevent transmission in unsecure transactions, and provided with a vendor defined expiration date, to force re-establishment of a credit relationship for inactive client users. If a cookie is found with a matching domain and path 58 the client browser adds the corresponding cookie data to the HTTP URL request message 60 that then is issued to the URL specified server 62. If a cookie is not found or has expired, the URL request message without a cookie is sent to the URL specified server 62.

Detailed Description Text (33):
A secure HTTP transaction will typically not be specified by the first URL of a redirection URL. Consequently, the redirection URL is issued to the sponsor server and a redirection message and second URL will be returned to the client browser 54. Preferably, the second URL specifies a secure transaction request and a server that can support secure transactions.

Detailed Description Text (34):
Alternately, the URL referenced server may refuse or fail the negotiation for a secure transaction with the client browser. In this case, the purchase transaction must be refused or proceed to be handled by the client browser and server in a conventional unsecure manner 57. However, since any cookie stored by the client browser for the referenced server and path is marked secure, the cookie is not sent by the client browser as part of any unsecure HTTP transaction with the URL referenced server.

Detailed Description Text (41):
Independent of whether the secure purchase algorithm of the present invention is implemented as an external CGI program or internal modification of the server application itself, the initial substantive action by the HTTPd server application is to determine whether a URL received in a secure transaction with a client browser references a purchasable product 64. The initial parsing of the URL by the HTTPd server application will determine whether a secure purchase transaction CGI program is to be executed by the HTTPd server or whether the "purchase" key word is embedded in the URL. Where neither effective product reference exists in the URL, the URL is further processed by the HTTPd server application in a conventional manner typically for the purpose of serving a Web page to the client browser 66.

Detailed Description Text (42):
Where a product is referenced by the URL, a determination is then made as to whether a cookie is provided as part of the HTTP message providing the received URL 68. Where no cookie is associated with the URL, the submission of the URL is taken to imply a request to establish a purchasing arrangement with the vendor server. Thus, the server system 16 replies to the URL by returning a new account form to the client browser 70. This form may request whatever information is deemed appropriate by the vendor in order to establish an open purchase arrangement with the vendor. Typically, the information requested includes a name, password, credit card number,

type of credit card, expiration date, and credit card billing address.

Detailed Description Text (43):
Once the client user has filled out the form, the client browser submits the form contents to the server system 16 for evaluation 72. The information provided by the client user may be automatically verified with the applicable credit card issuer or agent 74 to determine whether a valid account may be established for the client user. Should this credit check fail, the server system 16 preferably provides a form response to the client browser refusing the purchase transaction 76. Where the credit check succeeds, the server system 16 preferably opens a new account record for the client user 78. In addition, the server system 16 creates an initial cookie that encodes at least a client user identification code (ID) and the password submitted in connection with the new account form 72.

Detailed Description Text (44):
In an alternate preferred embodiment of the present invention, the cookie generated 78 not only encodes a client user ID and password, but also encodes other identifying information that is sent by the client browser as part of the URL request message. Encoding this additional information can serve to uniquely or at least substantially associate the cookie with a specific combination of the client browser and client system 12. In addition, the cookie may be further encrypted utilizing any conventional private key encryption algorithm. The private key and other information utilized in the construction of the cookie is stored with the account record for the client user. The substantive contents of the cookie is not decodable anywhere outside of the server system 16. Consequently, copies of the cookies as stored by the client system 12 are essentially non-portable among other possible client systems or modifiable to allow client user impersonation.

Detailed Description Text (45):
Where a cookie is provided 68 with the URL request issued by the client browser, the cookie is utilized to perform a database look-up to identify a client user account record. Regardless of whether the cookie has been encrypted, the cookie data can be utilized as the account reference for performing the database look-up of a client user record. The cookie data can then be validated against the information present in the account record. Where the cookie has been encrypted, the cookie can be decrypted utilizing the private key present in the account record and then validated against not only the other information stored within the account record but also present identifying information received directly from the client browser as part of the current HTTP transaction.

Detailed Description Text (46):
Where the cookies is determined invalid to due a failure to locate a current and valid account record corresponding to the cookie or in authenticating the cookie, a new account form can be provided to the client browser to establish or re-establish a credit relationship between the client user and vendor.

Detailed Description Text (47):
Where an account record is found and the cookie is authenticated 80, or where a new account has been successfully created 78, the server system 16 preferably then sends a confirmation form to the client browser 82. A new cookie, generated either in connection with the creation of an account record 78 or, where the cookie encodes a generational identifier that inherently changes over time and is potentially sequence specific, following validation of the received cookie 80, is provided by the server system 16 to the client browser in connection with the return of the confirmation form to the client browser. Even if a new cookie is not generated, a cookie is nonetheless preferably still set through an HTTP response to the client browser to update the expiration date associated with the cookie as held by the client browser. In all events, the cookie is marked secure.

Detailed Description Text (48):
In response, the client browser preferably displays the confirmation form on the client system 12 while recording the new or updated cookie in the client side storage provided by the client browser application 84. In a preferred embodiment of the present invention, the confirmation form provides an order summary sufficient to permit the client user to determine whether to confirm or cancel the order. The

client user completes and submits the form by selecting either to accept or cancel the order 86. Where, in an alternate embodiment, the confirmation form provides for accepting, cancelling and deferring purchase of individual products summarized on the confirmation form, the client user completes these choices prior to submitting the form as accepted as annotated or cancelled in its entirety. Assuming that the order is confirmed or at least accepted as annotated, the server operates from the confirmation data provided by the submitted form to update the client user's account record 87 and process the order generally in a conventional manner to provide for the delivery of the selected product to the client user 88.

CLAIMS:

1. A method of performing a purchase transaction between a client browser and a merchant server over a general purpose computer network comprising the steps of:

a) establishing a persistent predetermined coded identifier on a client browser corresponding to an account record stored by a merchant server;

b) providing for the serving of a Web page including a predetermined URL identifying a purchasable product or service to said client browser, said predetermined URL including a reference to said persistent predetermined coded identifier;

c) receiving said predetermined URL, including said persistent predetermined coded identifier, by said merchant server;

d) validating said predetermined coded identifier against said account record; and

e) recording the identity of said purchasable product or service as derived from said predetermined URL by said merchant server.

3. A method of claim 2 wherein said persistent predetermined identifier is stored in a secure manner by said client browser and communicated to said merchant server only through a secure network communications transaction.

4. The method of claim 3 wherein said persistent predetermined identifier is stored in an encrypted state by said client browser and includes data specific to said client browser so as to secure said predetermined identifier to said client browser.

5. The method of claim 4 wherein said process includes the step of confirming with said client browser the purchase of said purchasable product or service.

6. A method of performing trans-Internet purchase transactions between client browsers and merchant vendors, said method comprising the steps of:

a) providing for a predetermined Web page to be served to a client browser with said predetermined Web page identifying a purchasable item and including a corresponding purchase transaction URL;

b) receiving said corresponding purchase transaction URL and predetermined persistent cookie data previously stored by a merchant vendor on said client browser where said predetermined persistent cookie data is selected by said corresponding purchase transaction URL;

c) determining the identity of said purchasable item and from said corresponding purchase transaction URL; and

d) securely authenticating said client browser based on said predetermined persistent cookie data.

7. The method of claim 6 further comprising the steps of:

a) obtaining a confirmation from said client browser of the purchase selection of said purchasable item; and

b) recording the confirmed purchase selection of said purchasable item.

8. The method of claim 7 further comprising the step of providing a redirection message to said client browser to cause a client request for said predetermined Web page to be issued by said client browser.

9. The method of claim 8 wherein said step of obtaining a confirmation from said client browser includes optionally obtaining a personal identification number and a ship-to address for said purchasable item.

11. A method of presenting an electronic catalogue of purchasable items to a client browser wherein at least one merchant vendor is represented in the electronic catalogue, said method comprising the steps of:

a) serving a Web page of an electronic catalogue to a client browser, said Web page including identifications of a plurality of purchasable items, each one of said plurality of purchasable item having an associated URL embedded in said Web page;

b) receiving, in response to a single client browser selection, a predetermined URL request from said client browser including predetermined client environment data including predetermined persistent cookie data specifically corresponding to said predetermined URL;

c) validating said client browser and identifying a predetermined one of said plurality of purchasable items from said predetermined URL; and

d) serving a confirmation form to said client browser that requires a maximum of a single selection to accept and conclude the purchase of said predetermined one of said plurality of purchasable items.

12. The method of claim 11 wherein the Web page server is or is acting as an agent or proxy for a merchant vendor, said method further comprising the steps of:

a) identifying said client browser as representing a new account with respect to a merchant vendor;

b) establishing a credit relationship with said client browser on half of said merchant vendor; and

c) storing predetermined persistent cookie data, encoded to identify said client browser to said merchant vendor, on said client browser.

13. The method of claim 12 further comprising the steps of:

a) determining from said predetermined URL request or said predetermined client environment data an identification of said Web page; and

b) providing a redirection message including said identification of said Web page to said client browser following the step of serving said confirmation form to said client browser.

15. The method of claim 14 wherein said step of establishing a credit relationship with said client browser includes identification of an email address of said user of said client browser, said method further comprising the step of issuing an email confirmation of a purchase made by said client browser to said email address of said user.

16. A method of enabling purchase transactions for individual items from a plurality of merchant vendors through a common Web page, said method comprising the steps of:

a) embedding a first URL, associated with a purchasable item, in a Web page that is served from a first server to a client browser, said first URL referencing a second server;

b) providing for the storage of first persistent cookie data by said client browser and of a first database record by said second server, said first persistent cookie data corresponding to said first database record as stored by said second server;

c) receiving by said second server a first URL request corresponding to the client browser selection of said first URL;

d) receiving by said second server said first persistent cookie data;

e) validating said first persistent cookie data against said first database record;

f) identifying said purchasable item from said first URL request;

g) obtaining confirmation of the purchase of said purchasable item from said client browser; and

h) providing for said client browser to issue a second URL request to said first server to be served with said Web page.

19. The method of claim 18 wherein said step of obtaining confirmation of the purchase of said purchasable item from said second server includes said second server providing a ship-to address obtained from said client browser, said first database record, or said second server for the shipment of said purchasable item.

20. The method of claim 19 wherein said step of obtaining confirmation of the purchase of said purchasable item from said second server includes said client browser providing a personal identification number to said second server to authenticate the user of said client browser.

21. The method of claim 20 wherein said step of providing for said client browser to issue a second URL request to said first server includes providing new first persistent cookie data to said client browser for storage, said second server storing a new first database record corresponding to said new first persistent cookie data.